

ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention	Managing a Secure Environment Using a Chipset in Isolated Execution Mode
-------------------------------	---

Application Number : 09/540613



Confirmation Number: 2175

First Named Applicant: Carl Ellison

Attorney Docket Number: 42P08628

Art Unit: 2134

Examiner: Ellen Tran

Search string: (20010027511 or 20020007456 or 20020023032 or 20020147916 or 20020166061 or 20020169717 or 20030074548 or 20030115453 or 20030126442 or 20030126453 or 20030159056 or 20030188179 or 20030196085 or 20040117539 or 3699532 or 3996449 or 4207609 or 4319233 or 4403283 or 4419724 or 4430709 or 4621318 or 4802084 or 4975836 or 5187802 or 5230069 or 5237616 or 5287363 or 5295251 or 5361375 or 5469557 or 5506975 or 5555385 or 5555414 or 5560013 or 5564040 or 5574936 or 5582717 or 5604805 or 5633929 or 5668971 or 5684948 or 5706469 or 5740178 or 5752046 or 5809546 or 5825880 or 5919257 or 5935242 or 5935247).pn

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
EC	1	20010027511	2001-10-04	Wakabayashi, Masaki , et al.		711	163
	2	20020007456	2002-01-17	Peinado, Marcus , et al.		713	164
	3	20020023032	2002-02-21	Pearson, Siani L., et al.		705	35
	4	20020147916	2002-10-10	Strongin, Geoffrey S., et al.		713	193
	5	20020166061	2002-11-07	Falik, Ohad , et al.		713	200
	6	20020169717	2002-11-14	Challener, David C.		705	40
	7	20030074548	2003-04-17	Cromer, Daryl C., et al.		713	1
	8	20030115453	2003-06-19	Grawrock, David W.		713	155
✓	9	20030126442	2003-07-03	Glew, Andrew F., et al.		713	170

Best Available Copy

CLASS SOBUT

ECT	10	20030126453	2003-07-03	Glew, Andrew F., et al.	713	193	
	11	20030159056	2003-08-21	Cromer, Daryl C., et al.	713	193	
	12	20030188179	2003-10-02	Challener, David C., et al.	713	193	
	13	20030196085	2003-10-16	Lampson, Butler W., et al.	713	161	
	14	20040117539	2004-06-17	Bennett, Steve , et al.	711	6	
	15	3699532	1972-10-17	Schaffer, Harry G., et al.	710	48	
	16	3996449	1976-12-07	Attanasio, Clement R., et al.	235	431	
	17	4207609	1980-06-10	Luiz, Fernando A., et al.	710	38	
	18	4319233	1982-03-09	Matsuoka, Michihiro , et al.	346	622	
	19	4403283	1983-09-06	Myntti, Jon N., et al.	711	2	
	20	4419724	1983-12-06	Branigin, Michael H., et al.	710	108	
	21	4430709	1984-02-07	Schleupen, Richard , et al.	711	163	
	22	4621318	1986-11-04	Maeda, A.		364	200
	23	4802084	1989-01-31	Ikegaya, Hiroshi , et al.	711	6	
	24	4975836	1990-12-04	Hirosawa, Toshio , et al.	718	100	
	25	5187802	1993-02-16	Inoue, Taro , et al.	718	107	
	26	5230069	1993-02-16	Brelsford, David P., et al.	718	100	
	27	5237616	1993-08-17	Abraham, Dennis G., et al.	718	193	
	28	5287363	1994-02-15	Wolf, Paul I., et al.	714	718	
	29	5295251	1994-03-15	Wakui, Fujio , et al.	718	1	
	30	5361375	1994-11-01	Ogi, Yoshifumi	716	1	
	31	5469557	1995-11-21	Salt, Tom , et al.	711	163	
	32	5506975	1996-04-09	Onodera, Osama	714	1	
	33	5555385	1996-09-10	Osisek, Damian L.	711	1	
	34	5555414	1996-09-10	Hough, Roger E., et al.	710	261	
	35	5560013	1996-09-24	Scalzi, Casper A., et al.	717	138	
	36	5564040	1996-10-08	Kubala, Jeffrey P.	711	173	

CLASS SUBCLASS

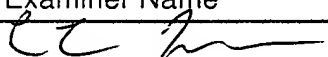
ECT	37	5574936	1996-11-12	Ryba, Edward G., et al.	712	30	
	38	5582717	1996-12-10	Di Santo, Dennis E.	210	86	
	39	5604805	1997-02-18	Brands, Stefanus A.	360	30	
	40	5633929	1997-05-27	Kaliski, Jr., Burton S.	711	111	
	41	5668971	1997-11-16	Neufeld, E. D.	713	200	
	42	5684948	1997-11-04	Johnson, James S., et al.	710	240	
	43	5706469	1998-01-06	Kobayashi, Souichi	714	722	
	44	5740178	1998-04-14	Jacks, Steven A., et al.	713	200	
	45	5752046	1998-05-12	Oprescu, Florin , et al.	713	300	
	46	5809546	1998-09-15	Greenstein, Paul G., et al.	711	164	
	47	5825880	1998-10-20	Sudia, Frank W., et al.	713	180	
	48	5919257	1999-07-06	Trostle, Jonathan	713	200	
	49	5935242	1999-08-10	Madany, Peter W., et al.	713	1	
✓	50	5935247	1999-08-10	Pai, Hsin-Ying , et al.	713	200	

Remarks

Note: Remarks are not for responding to an office action.

Part 1 of 2 IDSes.

Signature

Examiner Name	Date
	29 AUG 2005

ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention	Managing a Secure Environment Using a Chipset in Isolated Execution Mode
-------------------------------	---

Application Number : 09/540613



Confirmation Number: 2175

First Named Applicant: Carl Ellison

Attorney Docket Number: 42P08628

Art Unit: 2134

Examiner: Ellen Tran

Search string: (3996449 or 5935247 or 5944821 or 5956408 or 5978475 or 6035374 or 6044478 or 6088262 or 6093213 or 6108644 or 6131166 or 6173417 or 6175924 or 6188257 or 6199152 or 6275933 or 6282650 or 6327652 or 6378068 or 6397379 or 6529909 or 6560627 or 6609199 or 6615278 or 6651171 or 6678825 or 6684326),pn

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
ECT	1	3996449	1976-12-07	Attanasio, Clement R., et al.		235	431
	2	5935247	1999-08-10	Pai, Hsin-Ying , et al.		713	200
	3	5944821	1999-08-31	Angelo, Michael F.		364	200
	4	5956408	1999-09-21	Arnold, Todd W.			
	5	5978475	1999-11-02	Schneier, Bruce , et al.		713	177
	6	6035374	2000-03-07	Panwar, Ramesh , et al.		711	118
	7	6044478	2000-03-28	Green, Daniel W.		714	42
	8	6088262	2000-07-11	Nasu, Hiroaki		365	188, 01
	9	6093213	2000-07-25	Favor, John G., et al.		703	27
	10	6108644	2000-08-22	Goldschlag, David M., et al.		705	69
	11	6131166	2000-10-10	Wong-Isley, Becky		713	300
	12	6173417	2001-01-09	Merrill, John W.		714	15
✓	13	6175924	2001-01-16	Arnold, Todd W.	713	713	189

ECT	14	6188257	2001-02-13	Buer, Mark L.		327	143
	15	6199152	2001-03-06	Kelly, Edmund J., et al.		711	207
	16	6275933	2001-08-14	Fine, Michael , et al.		713	2
	17	6282650	2001-08-28	Davis, Derek L.		713	176
	18	6327652	2001-12-04	England, Paul , et al.		713	2
	19	6378068	2002-04-23	Foster, Mark J.		713	1
	20	6397379	2002-05-28	Yates, Jr., John S., et al.		717	140
	21	6529909	2003-03-04	Bowman-Amuah, Michel K.		707	10
	22	6560627	2003-05-06	McDonald, Michael F., et al.		718	103
	23	6609199	2003-08-19	DeTreville, John		713	172
	24	6615278	2003-09-02	Curtis, Bryce A.		719	316
	25	6651171	2003-11-18	England, Paul , et al.		713	193
	26	6678825	2004-01-13	Ellison, Carl M., et al.		713	200
✓	27	6684326	2004-01-27	Cromer, Daryl C., et al.	✓	713	2

ECT

Remarks

Note: Remarks are not for responding to an office action.

Part 2 of 2 electronic IDSs.

Signature

Examiner Name	Date
CT [Signature]	29 AUG 2004



09/540,613

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Carl M. Ellison et al.

Application No.: 09/540,613

Docket No.: P8628

Filed: 03/31/00

For: MANAGING A SECURE
ENVIRONMENT USING A CHIPSET
IN ISOLATED EXECUTION MODE

Examiner: Ellen C. Tran

Art Unit: 2134

Phone No.: (703) 305-8917

CROSS REFERENCE TO RELATED APPLICATIONS

COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir:

Applicants hereby cross-reference the following related patents and patent applications, which are all assigned to the same assignee as the present patent application.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on:

9-21-04

Date of Deposit

Kristin A. Morrow

Name of Person Mailing Correspondence

Kristin A. Morrow

Signature

Date

9-21-04

09/540,613

ECT

Reference No.	Application Serial No.	Patent No.	Title
1	09/672,603		Controlling Accesses To Isolated Memory Using A Memory Controller For Isolated Execution
2	09/822,986		Checking File Integrity Using Signature Generated In Isolated Execution
3	09/538,951		Platform And Method For Issuing And Certifying A Hardware-Protected Attestation Key
4	09/539,344		Managing A Secure Platform Using A Hierarchical Executive Architecture In Isolated Execution Mode
5	09/668,585		Managing A Secure Platform Using A Hierarchical Executive Architecture In Isolated Execution Mode
6	09/541,108		Platform And Method For Remote Attestation Of A Platform
7	09/540,612		Platform And Method For Generating And Utilizing A Protected Audit Log
8	09/540,946		Protecting Software Environment In Isolated Execution
9	09/668,610		Protecting Software Environment In Isolated Execution
10	09/538,954		Generating Isolated Bus Cycles For Isolated Execution
11	09/539,348	6,760,441	Generating A Key Hierarchy For Use In An Isolated Execution Environment
12	09/541,477	6,507,904	Isolated Instructions For Isolated Execution
13	09/540,611		Managing Accesses In A Processor For Isolated Execution
14	09/540,613		Managing A Secure Environment Using A Chipset In Isolated Execution Mode
15	09/668,408		Managing A Secure Environment Using A Chipset In Isolated Execution Mode
16	09/541,667		Attestation Key Memory Device And Bus
17	09/672,602		Attestation Key Memory Device And Bus
18	09/618,738	6,678,825	Controlling Access To Multiple Isolated Memories In An Isolated Execution Environment
19	09/618,489	6,633,963	Controlling Access To Multiple Memory Zones In An Isolated Execution Environment
20	10/683,542		Controlling Access To Multiple Memory Zones In An Isolated Execution Environment
21	09/618,659		Resetting A Processor In An Isolated Execution Environment
22	09/751,586		Resetting A Processor In An Isolated Execution Environment

EE

29 AUG '05

09/540,613

It may be noted that the above list includes the present application, and the above list partially overlaps the cross-reference to related applications that was filed earlier.

If there are any questions that may be cleared up in a telephone interview, the Examiner is invited to call the undersigned at (512) 732-3927.

Respectfully submitted,

Dated: 9/20/04

MParré
Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026



Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)				Application Number	09/540,613
				Filing Date	March 31, 2000
				First Named Inventor	Carl M. Ellison
				Art Unit	2134
				Examiner Name	Ellen C. Tran
				Attorney Docket Number	42390P8628
Sheet	1	of	1		

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.	Document Number	Publication Date or Issue Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code ¹ (if known)			
ECT ↓	1	US-5,950,221	09-07-1999	Draves et al.	
	2	US-5,898,883	04-27-1999	Fujii et al.	
	3	US-5,668,971	09-16-1997	Neufeld	
	4	US-5,522,075	05-28-1996	Robinson et al.	
	5	US-5,303,378	04-12-1994	Cohen	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Country Code ² - Number - Kind Code ³ (if known)			

Examiner Signature		Date Considered	29 AUG 2005
-----------------------	--	--------------------	-------------

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

¹Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. Applicant is to place a check mark here if English language translation is attached.

Based on PTO/SB/08A (08-03) as modified by Blakely, Solokoff, Taylor & Zafman (wtr) 08/11/2003.

Send To: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Substitute for form 1449A/PTO
**INFORMATION DISCLOSURE
 STATEMENT BY APPLICANT**
 (Use as many sheets as necessary)



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it appears to have a valid OMB control number.

PTO/SB/04M (10-01)
 Approved for use through 10/14/2002. OMB 051-0031
 US Patent & Trademark Office U.S. DEPARTMENT OF COMMERCE

Complete if Known	
Application Number	09/540,611
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	2134
Examiner Name	Tran, Ellen

Sheet 1 of 2

Attorney Docket No: 42P08112

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T ²
ECT	EP-EP0892521	01/20/1999	Zamek, Steven			
	EP-EP1055989	11/29/2000	Proudlar, Graeme J., et al.			
	EP-EP1056014	11/29/2000	Proudlar, Graeme J., et al.			
	WO-WO0201794	01/03/2002	Ellison, Carl			
	WO-WO02060121	08/01/2002	Grawrock, David W.			
	WO-WO03058412	07/17/2003	Glew, Andrew, et al.			
	WO-WO9812620	03/26/1998	Nishiuchi, Taiki, et al.			
✓	WO-WO9918511	04/15/1999	Edrich, David R.			

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
ECT		COULOURIS, GEORGE, et al., "Distributed Systems, Concepts and Designs", 2nd Edition, (1994), 422-424	
		CRAWFORD, JOHN, "Architecture of the Intel 80386", <u>Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD '86)</u> , (October 6, 1986), 155-160	
		FABRY, R.S., "Capability-Based Addressing", <u>Fabry, R.S., "Capability-Based Addressing"</u> , Communications of the ACM, Vol. 17, No. 7, (July 1974), 403-412	
		FRIEDER, GIDEON, "The Architecture And Operational Characteristics of the VMX Host Machine", <u>The Architecture And Operational Characteristics of the VMX Host Machine, IEEE</u> , (1982), 9-16	
		INTEL CORPORATION, "IA-64 System Abstraction Layer Specification", <u>Intel Product Specification, Order Number 245359-001</u> , (01/2000), 1-112	
		INTEL CORPORATION, "Intel IA-64 Architecture Software Developer's Manual", <u>Volume 2: IA-64 System Architecture, Order Number 245318-001</u> , (01/2000), i, ii, 5.1-5.3, 11.1-11.8, 11.23-11.26	
		MENEZES, ALFRED J., et al., "Handbook of Applied Cryptography", <u>CRC Press Series on Discrete Mathematics and Its Applications</u> , Boca Raton, FL, XP002165287, ISBN 0849385237, (Oct. 1998), 403-405, 508-515, 570	
		NANBA, S., et al., "VM/4: ACOS-4 Virtual Machine Architecture", <u>VM/4: ACOS-4 Virtual Machine Architecture, IEEE</u> , (1985), 171-178	
		RSA SECURITY, "Hardware Authenticators", <u>www.rsasecurity.com/node.asp?id=1158</u> , 1-2	
		RSA SECURITY, "RSA SecurID Authenticators", <u>www.rsasecurity.com/products/securid/datasheets/SID_DS_0103.pdf</u> , 1-2	
✓		RSA SECURITY, "Software Authenticators", <u>www.rsasecurity.com/node.asp?id=1313</u> , 1-2	

EXAMINER

ECT

DATE CONSIDERED

9 Aug 2004

Substitute Disclosure Statement Form (PTO-1449)
 * EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 800. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional) Applicant is to place a check mark here if English language Translation is attached

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substituted for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known	
	Application Number	09/540,611
	Filing Date	March 31, 2000
	First Named Inventor	Ellison, Carl
	Group Art Unit	2134
	Examiner Name	Tran, Ellen
Sheet 2 of 2	Attorney Docket No: 42P08112	

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T*
ECT		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithm, and Source Code in C", Wiley, John & Sons, Inc., XP002939871; ISBN 0471117099, (Oct. 1995), 47-52	
↓		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithm, and Source Code in C", Wiley, John & Sons, Inc., XP002138607; ISBN 0471117099, (Oct. 1995), 56-65	
↓		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Wiley, John & Sons, Inc., XP0021111449; ISBN 0471117099, (Oct. 1995), 169-187	
↓		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition; Wiley, John & Sons, Inc., XP002251738; ISBN 0471128457, (Nov. 1995), 28-33; 176-177; 216-217; 461-473; 518-522	

EXAMINER

DATE CONSIDERED

1/16/04

Substitute Disclosure Statement Form (PTO-1449)

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). Applicant to place a check mark here if English language Translation is attached.



ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

Title of Invention	Managing Accesses in a Processor for Isolated Execution																																																																																																										
<p>Application Number: 09/540611</p> <p>Confirmation Number: 2172</p> <p>First Named Applicant: Carl Ellison</p> <p>Attorney Docket Number: 42P08112</p> <p>Art Unit: 2134</p> <p>Examiner: Ellen Tran</p> <p>Search string: (3699532 or 4207609 or 4319233 or 4403283 or 4419724 or 5237616 or 5287363 or 5560013 or 5604805 or 5633929 or 5668971 or 5684948 or 5706469 or 5740178 or 5752046 or 5809546 or 5825880 or 5919257 or 5935242 or 5935247 or 6035374 or 6093213 or 6108644 or 6131166 or 6199152 or 6327652 or 6397379 or 6529909 or 6560627 or 6609199 or 6615278 or 6651171 or 6684326).pn.</p>																																																																																																											
<h3>US Patent Documents</h3> <p>Note: Applicant is not required to submit a paper copy of cited US Patent Documents</p> <table border="1"><thead><tr><th>init</th><th>Cite.No.</th><th>Patent No.</th><th>Date</th><th>Patentee</th><th>Kind</th><th>Class</th><th>Subclass</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>1</td><td>3699532</td><td>1972-10-17</td><td>Schaffer, Harry G., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>2</td><td>4207609</td><td>1980-06-10</td><td>Luiz, Fernando A., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>3</td><td>4319233</td><td>1982-03-09</td><td>Matsuoka, Michihiro , et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>4</td><td>4403283</td><td>1983-09-06</td><td>Myntti, Jon N., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>5</td><td>4419724</td><td>1983-12-06</td><td>Branigin, Michael H., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>6</td><td>5237616</td><td>1993-08-17</td><td>Abraham, Dennis G., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>7</td><td>5287363</td><td>1994-02-15</td><td>Wolf, Paul I., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>8</td><td>5560013</td><td>1996-09-24</td><td>Scalzi, Casper A., et al.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>9</td><td>5604805</td><td>1997-02-18</td><td>Brands, Stefanus A.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>10</td><td>5633929</td><td>1997-05-27</td><td>Kaliski, Jr., Burton S.</td><td></td><td></td><td></td></tr><tr><td><input type="checkbox"/></td><td>11</td><td>5668971</td><td>1997-11-16</td><td>Neufeld, E. D.</td><td></td><td></td><td></td></tr><tr><td><input checked="" type="checkbox"/></td><td>12</td><td>5684948</td><td>1997-11-04</td><td>Johnson, James S., et al.</td><td></td><td></td><td></td></tr></tbody></table>				init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass	<input checked="" type="checkbox"/>	1	3699532	1972-10-17	Schaffer, Harry G., et al.				<input type="checkbox"/>	2	4207609	1980-06-10	Luiz, Fernando A., et al.				<input type="checkbox"/>	3	4319233	1982-03-09	Matsuoka, Michihiro , et al.				<input type="checkbox"/>	4	4403283	1983-09-06	Myntti, Jon N., et al.				<input type="checkbox"/>	5	4419724	1983-12-06	Branigin, Michael H., et al.				<input type="checkbox"/>	6	5237616	1993-08-17	Abraham, Dennis G., et al.				<input type="checkbox"/>	7	5287363	1994-02-15	Wolf, Paul I., et al.				<input type="checkbox"/>	8	5560013	1996-09-24	Scalzi, Casper A., et al.				<input type="checkbox"/>	9	5604805	1997-02-18	Brands, Stefanus A.				<input type="checkbox"/>	10	5633929	1997-05-27	Kaliski, Jr., Burton S.				<input type="checkbox"/>	11	5668971	1997-11-16	Neufeld, E. D.				<input checked="" type="checkbox"/>	12	5684948	1997-11-04	Johnson, James S., et al.			
init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass																																																																																																				
<input checked="" type="checkbox"/>	1	3699532	1972-10-17	Schaffer, Harry G., et al.																																																																																																							
<input type="checkbox"/>	2	4207609	1980-06-10	Luiz, Fernando A., et al.																																																																																																							
<input type="checkbox"/>	3	4319233	1982-03-09	Matsuoka, Michihiro , et al.																																																																																																							
<input type="checkbox"/>	4	4403283	1983-09-06	Myntti, Jon N., et al.																																																																																																							
<input type="checkbox"/>	5	4419724	1983-12-06	Branigin, Michael H., et al.																																																																																																							
<input type="checkbox"/>	6	5237616	1993-08-17	Abraham, Dennis G., et al.																																																																																																							
<input type="checkbox"/>	7	5287363	1994-02-15	Wolf, Paul I., et al.																																																																																																							
<input type="checkbox"/>	8	5560013	1996-09-24	Scalzi, Casper A., et al.																																																																																																							
<input type="checkbox"/>	9	5604805	1997-02-18	Brands, Stefanus A.																																																																																																							
<input type="checkbox"/>	10	5633929	1997-05-27	Kaliski, Jr., Burton S.																																																																																																							
<input type="checkbox"/>	11	5668971	1997-11-16	Neufeld, E. D.																																																																																																							
<input checked="" type="checkbox"/>	12	5684948	1997-11-04	Johnson, James S., et al.																																																																																																							

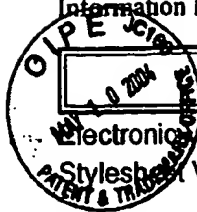
APP_ID=09540611

Page 1 of 2

<input checked="" type="checkbox"/>	13	5706469	1998-01-06	Kobayashi, Souichi
<input type="checkbox"/>	14	5740178	1998-04-14	Jacks, Steven A., et al.
<input type="checkbox"/>	15	5752046	1998-05-12	Oprescu, Florin , et al.
<input type="checkbox"/>	16	5809546	1998-09-15	Greenstein, Paul G., et al.
<input type="checkbox"/>	17	5825880	1998-10-20	Sudia, Frank W., et al.
<input type="checkbox"/>	18	5919257	1999-07-06	Trostle, Jonathan
<input type="checkbox"/>	19	5935242	1999-08-10	Madany, Peter W., et al.
<input type="checkbox"/>	20	5935247	1999-08-10	Pai, Hsin-Ying , et al.
<input type="checkbox"/>	21	6035374	2000-03-07	Panwar, Ramesh , et al.
<input type="checkbox"/>	22	6093213	2000-07-25	Favor, John G., et al.
<input type="checkbox"/>	23	6108644	2000-08-22	Goldschlag, David M., et al.
<input type="checkbox"/>	24	6131166	2000-10-10	Wong-Isley, Becky
<input type="checkbox"/>	25	6199152	2001-03-06	Kelly, Edmund J., et al.
<input type="checkbox"/>	26	6327652	2001-12-04	England, Paul , et al.
<input type="checkbox"/>	27	6397379	2002-05-28	Yates, Jr., John S., et al.
<input type="checkbox"/>	28	6529909	2003-03-04	Bowman-Amuah, Michel K.
<input type="checkbox"/>	29	6560627	2003-05-06	McDonald, Michael F., et al.
<input type="checkbox"/>	30	6609199	2003-08-19	DeTreville, John
<input type="checkbox"/>	31	6615278	2003-09-02	Curtis, Bryce A.
<input checked="" type="checkbox"/>	32	6651171	2003-11-18	England, Paul , et al.
<input checked="" type="checkbox"/>	33	6684326	2004-01-27	Cromer, Daryl C., et al.

Signature

Examiner Name	Date
<i>E. J. [Signature]</i>	1 Apr 04



ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic version v18
 Stylesheet Version v18.0

Title of Invention

Managing a Secure Environment Using a Chipset in Isolated Execution Mode

Application Number: 09/540613

Confirmation Number: 2175

First Named Applicant: Carl Ellison

Attorney Docket Number: 42P08628

Art Unit: Unknown

Examiner: Unknown Unknown

Search string: (20030018892 or 4162536 or 4247905 or 4276594 or 4307447 or 4319323 or 4347565 or 4759064 or 4795893 or 4825052 or 4907270 or 4907272 or 4910774 or 5007082 or 5139760 or 5317705 or 5319760 or 5434999 or 5437033 or 5442645 or 5459867 or 5504922 or 5511217 or 5522075 or 5528231 or 5533126 or 5566323 or 5606617 or 5720609 or 5721222 or 5737604 or 5796835 or 5825875 or 5854913 or 5867577 or 5900606 or 5901225 or 5903752 or 5970147 or 6061794 or 6075938 or 6092095 or 6115816 or 6182089 or 6212635 or 6222923 or 6252650 or 6269392 or 6272637 or 6308270 or 6314409 or 6330670 or 6357004 or 6363485 or 6374286 or 6374317 or 6378072 or 6389537 or 6397242 or 6412035 or 6421702 or 6435416 or 6445797 or 6463535 or 6463537 or 6507904 or 6535988 or 6557104 or 6633963 or 6633981).pn.

RECEIVED

MAY 13 2004

Technology Center 2100

09/540613

US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

Init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
<input checked="" type="checkbox"/>	1	20030018892	2003-01-23	Tello, Jose			
<input checked="" type="checkbox"/>	2	4162536	1979-07-24	Morley, Richard E.			
<input checked="" type="checkbox"/>	3	4247905	1981-01-27	Yoshida, Yukihiro , et al.		711	166
<input checked="" type="checkbox"/>	4	4276594	1981-08-30	Morley, Richard E.			
<input checked="" type="checkbox"/>	5	4307447	1981-12-22	Provanzano, Salvatore R., et al.			
<input checked="" type="checkbox"/>	6	4319323	1982-03-09	Ermolovich, Thomas R., et al.			
<input checked="" type="checkbox"/>	7	4347565	1982-08-31	Kaneda, Saburo , et al.			
<input checked="" type="checkbox"/>	8	4759064	1988-07-19	Chaum,			
<input checked="" type="checkbox"/>	9	4795893	1989-01-03	Ugon, Michael			
<input checked="" type="checkbox"/>	10	4825052	1989-04-25	Chemin, Francois , et al.			
<input checked="" type="checkbox"/>	11	4907270	1990-03-08	Hazard, Michel			

12	4907272	1990-03-06	Hazard, Michel
13	4910774	1990-03-20	Barakat, Simon
14	5007082	1991-04-09	Cummins, Mary T.
15	5139760	1994-06-07	Mason, Andrew H., et al.
16	5317705	1994-05-31	Gannon, Patrick M., et al.
17	5319760	1994-06-07	Mason, Andrew H., et al.
18	5434999	1995-07-18	Goire, Christian , et al.
19	5437033	1995-07-25	Inoue, Taro , et al.
20	5442645	1995-08-15	Ugon, Michel , et al.
21	5459867	1995-10-17	Adams, Phillip M., et al.
22	5504922	1996-04-02	Seki, Yukihiko , et al.
23	5511217	1996-04-23	Nakajima, Atsushi , et al.
24	5522075	1996-05-28	Robinson, Paul T., et al.
25	5528231	1996-06-18	Patarin, Jacques
26	5533126	1996-07-02	Hazard, Michel , et al.
27	5566323	1996-10-15	Ugon, Michel
28	5606617	1997-02-25	Brands, Stefanus A.
29	5720609	1998-02-24	Pfefferle, William C.
30	5721222	1998-02-24	Bernstein, Peter R., et al.
31	5737604	1998-04-07	Miller, David A., et al.
32	5796835	1998-08-18	Saada, Charles
33	5825875	1998-10-20	Ugon, Michel
34	5854913	1998-12-29	Goetz, John W., et al.
35	5867577	1999-02-02	Patarin, Jacques
36	5900606	1999-05-04	Rigal, Vincent
37	5901225	1999-05-04	Ireton, Mark A., et al.
38	5903752	1999-05-11	Dingwall, Thomas J., et al.
39	5970147	1999-10-19	Davis, Derek L., et al.
40	6061794	2000-05-09	Angelo, Michael E.
41	6075938	2000-06-13	Bugnon, Edouard , et al.
42	6092095	2000-07-18	Maytal, Benjamin
43	6115816	2000-09-05	Davis, Derek L.
44	6182089	2001-01-30	Ganapathy, Narayanan , et al.
45	6212635	2001-04-03	Reardon, David C.
46	6222923	2001-04-24	Schwenk, Joerg
47	6252650	2001-06-26	Nakaumra, Kouji
48	6269392	2001-07-31	Cotichini, Christian , et al.
49	6272637	2001-08-07	Little, Wendell L., et al.

713

194

<input checked="" type="checkbox"/>	50	6308270	2001-10-23	Guthery, Scott B., et al.
<input checked="" type="checkbox"/>	51	6314409	2001-11-06	Schneck, Paul B., et al.
<input checked="" type="checkbox"/>	52	6330670	2001-12-11	England, Paul, et al.
<input checked="" type="checkbox"/>	53	6357004	2002-03-12	Davis, Derek L.
<input checked="" type="checkbox"/>	54	6363485	2002-03-26	Adams, Carlisle
<input checked="" type="checkbox"/>	55	6374286	2002-04-16	Gee, John K., et al.
<input checked="" type="checkbox"/>	56	6374317	2002-04-16	Ajanovic, Jasmin, et al.
<input checked="" type="checkbox"/>	57	6378072	2002-04-23	Collins, Thomas, et al.
<input checked="" type="checkbox"/>	58	6389537	2002-05-14	Davis, Derek L., et al.
<input checked="" type="checkbox"/>	59	6397242	2002-05-28	Devine, Scott W., et al.
<input checked="" type="checkbox"/>	60	6412035	2002-06-25	Webber, Victor
<input checked="" type="checkbox"/>	61	6421702	2002-07-16	Gulick, Dale E.
<input checked="" type="checkbox"/>	62	6435416	2002-08-20	Slassi, Tarik
<input checked="" type="checkbox"/>	63	6445797	2002-09-03	McGough, Paul, et al.
<input checked="" type="checkbox"/>	64	6463535	2002-10-08	Drews, Paul C., et al.
<input checked="" type="checkbox"/>	65	6463537	2002-10-08	Tello, Jose A.
<input checked="" type="checkbox"/>	66	6507904	2003-01-14	Ellison, Carl M., et al.
<input checked="" type="checkbox"/>	67	6535988	2003-03-18	Poisner, David L.
<input checked="" type="checkbox"/>	68	6557104	2003-04-29	Vu, Son T., et al.
<input checked="" type="checkbox"/>	69	6633963	2003-10-14	Ellison, Carl M., et al.
<input checked="" type="checkbox"/>	70	6633981	2003-10-14	Davis, Derek L.

710	105
-----	-----

Remarks

Note: Remarks are not for responding to an office action.

Applicants, in accordance with their duty of disclosure under 37 CFR 1.56 and in accordance with 37 CFR 1.97(b)(3), hereby submit this Electronic Information Disclosure Statement citing U.S. Patent Documents for consideration by the Examiner. Pursuant to 37 CFR 1.97, the submission of this Electronic Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability. This Electronic Information Disclosure Statement is being filed prior to a substantive examination of the claims. Pursuant to 37 CFR 1.97(b), no fee should be required for the filing of this Electronic Information Disclosure Statement. In the event it is determined that a fee is due, please charge the fee to Deposit Account 02-2666. Applicants respectfully request that the cited documents be considered and that the form be initialed by the Examiner to indicate such consideration and a copy thereof be returned to Applicants' attorney of record.

Signature

EE Jan 9 AUG '04

Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability. This Electronic Information Disclosure Statement is being filed prior to a substantive examination of the claims. Pursuant to 37 CFR 1.97(b), no fee should be required for the filing of this Electronic Information Disclosure Statement. In the event it is determined that a fee is due, please charge the fee to Deposit Account 02-2666. Applicants respectfully request that the cited documents be considered and that the form be initialed by the Examiner to indicate such consideration and a copy thereof be returned to Applicants' attorney of record.

Signature

Examiner Name	Date
<i>EC</i>	7 AUG '09

Substitute for Form 1449A/PTO (Modified)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Complete if Known

Application Number	09/540,613
Filing Date	March 31, 2000
First Named Inventor:	Carl M. Ellison
Group Art Unit	2782
Examiner Name	Unassigned
Attorney Docket Number	042390P8628

Sheet 2 of 2

OTHER ART - NO PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
ECT		GOLDBERG, R., "Survey of virtual machine research," IEEE Computer Magazine 7(6), pp. 34-45, 1974.	
ECT		GUM, P.H., "System/370 Extended Architecture: Facilities for Virtual Machines," IBM J. Research Development, Vol 27, Number 6, pp. 530-544, November 1983	
ECT		ROSENBLUM, M. "Vmware's Virtual Platform: A Virtual Machine Monitor for Commodity PCs," Proceedings of the 11th Hotchips Conference, pp. 185-196, August 1999.	
ECT		LAWTON, K., "Running Multiple Operating Systems Concurrently on an IA32 PC Using Virtualization Techniques," http://www.plex86.org/research/paper.txt ; 11/29/1999; pp. 1-31.	

RECEIVED

NOV 25 2002

Technology Center 2100

Examiner Signature	<i>ECT</i>	Date Considered	27 JAN '04
--------------------	------------	-----------------	------------

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

¹Unique citation designation number. ²Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



Substitute for form 1449A/PTO
**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Use as many sheets as necessary)

Complete if Known

Application Number	09/540,613
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown

Sheet 1 of 2

Attorney Docket No: 42P08628

US PATENT DOCUMENTS

Examiner Initial*	USP Document Number	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	Filing Date If Appropriate
-------------------	---------------------	------------------	---	-------	----------	----------------------------

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T ²
ECF	EP-EP0892521	01/20/1999	Zamek, Steven			
	EP-EP0961193	12/01/1999	Laczko, Sr., Frank L.			
	EP-EP0965902	12/22/1999	Force, Gordon, et al.			
	EP-EP1055989	11/29/2000	Proudlar, Graeme J., et al.			
	EP-EP1056014	11/29/2000	Proudlar, Graeme J., et al.			
	EP-EP1085396	03/21/2001	Proudlar, Graeme J., et al.			
	WO-WO0021238	04/13/2000	Drews, Paul C.			
	WO-WO0163994	08/30/2001	Van Sant, Glen, et al.			
	WO-WO0201794	01/03/2002	Ellison, Carl			
	WO-WO02060121	08/01/2002	Grawrock, David W.			
	WO-WO03058412	07/17/2003	Glew, Andrew, et al.			
	WO-WO9524696	09/14/1995	Mooney, David M., et al.			
	WO-WO9812620	03/26/1998	Nishiuchi, Taiki, et al.			
	WO-WO9918511	04/15/1999	Edrich, David R.			
	WO-WO9965579	12/23/1999	Bond, Eugene T.			

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initial*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
ECF		COULOURIS, GEORGE, et al., "Distributed Systems, Concepts and Designs", 2nd Edition, (1994), 422-424	
		CRAWFORD, JOHN, "Architecture of the Intel 80386", <u>Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD '86)</u> , (October 6, 1986), 155-160	
		FABRY, R.S., "Capability-Based Addressing", Fabry, R.S., "Capability-Based Addressing," <u>Communications of the ACM</u> , Vol. 17, No. 7, (July 1974), 403-412	
		FRIEDER, GIDEON, "The Architecture And Operational Characteristics of the VMX Host Machine", <u>The Architecture And Operational Characteristics of the VMX Host Machine</u> , IEEE, (1982), 9-16	
		INTEL CORPORATION, "IA-64 System Abstraction Layer Specification", <u>Intel Product Specification</u> , Order Number 245359-001, (01/2000), 1-112	
		INTEL CORPORATION, "Intel IA-64 Architecture Software Developer's Manual", Volume 2: <u>IA-64 System Architecture</u> , Order Number 245318-001,	

EXAMINER

ECF

DATE CONSIDERED

18 MAR '05

Substitute Disclosure Statement Form (PTO-1442)

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 908. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional): Applicant is to place a check mark here if English language translation is attached



Substitute for form 1449A/PTO
**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Use as many sheets as necessary)

Complete if Known

Application Number	09/540,613
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Unknown

Sheet 2 of 2

Attorney Docket No: 42P08628

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
ECT		(01/2000), i, ii, 5.1-5.3, 11.1-11.8, 11.23-11.26	
		MENEZES, ALFRED J., et al., "Handbook of Applied Cryptography", <u>CRC Press Series on Discrete Mathematics and its Applications</u> , Boca Raton, FL, XP002165287, ISBN 0849385237, (Oct. 1996), 403-405, 506-515, 570	
		NANBA, S., et al., "VM/4: ACOS-4 Virtual Machine Architecture", <u>VM/4: ACOS-4 Virtual Machine Architecture</u> , IEEE, (1985), 171-178	
		RSA SECURITY, "Hardware Authenticators", www.rsasecurity.com/node.asp?id=1158 , 1-2	
		RSA SECURITY, "RSA SecurID Authenticators", www.rsasecurity.com/products/securid/datasheets/SID_DS_0103.pdf , 1-2	
		RSA SECURITY, "Software Authenticators", www.rsasecurity.com/node.asp?id=1313 , 1-2	
		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithm, and Source Code in C", <u>Wiley, John & Sons, Inc.</u> , XP002138607; ISBN 0471117099, (Oct. 1995), 56-65	
		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithms, and Source Code C", <u>Wiley, John & Sons, Inc.</u> , XP002111449; ISBN 0471117099, (Oct. 1995), 169-187	
		SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition; <u>Wiley, John & Sons, Inc.</u> , XP002251738; ISBN 0471128457, (Nov. 1995), 28-33; 176-177; 216-217; 461-473; 518-522	

EXAMINER

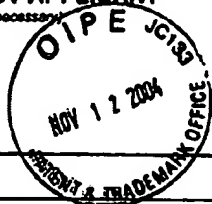
DATE CONSIDERED

18 MAR 05

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Sheet 1 of 2

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Approved for use through 10/31/2002, OMB 05-1-0001
US Patent & Trademark Office, U.S. DEPARTMENT OF COMMERCE

Complete if Known

Application Number	09/540,613
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Tran, Ellen

Attorney Docket No: 42P08628

US PATENT DOCUMENTS

Examiner Initial*	USP Document Number	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	Filing Date If Appropriate
-------------------	---------------------	------------------	---	-------	----------	----------------------------

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Foreign Document No	Publication Date	Name of Patentee or Applicant of cited Document	Class	Subclass	T ¹
ELF	DE-DE4217444	12/03/1992	Toyohisa, Imada, et al.			
	EP-EP0473913	03/11/1992	Farrell, Joel A.			
	EP-EP0961193	12/01/1999	Laczko, Sr., Frank L.			
	EP-EP1209563	05/29/2002	England, Paul, et al.	G06F	9/445	
	EP-EP1271277	01/02/2003	Behar, Yaachov			
	WO-WO0021238	04/13/2000	Drews, Paul C.			
	WO-WO0175564	10/11/2002	Herbert, Howard C., et al.			
	WO-WO02086684	10/31/2002	Proudler, Graeme J.			
	WO-WO0217555	02/28/2002	Ford, Warwick			

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initial*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ¹
ELF	✓	BRANDS, STEFAN, "Restrictive Blinding of Secret-Key Certificates", SPRINGER-VERLAG XP002201306, (1995), Chapter 3	
	✓	CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221	
	✓	COMPAQ COMPUTER CORPORATION, "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", XP002272822, (1/25/2001), 1-321	
	✓	DAVIDA, GEORGE I., et al., "Defending Systems Against Viruses through Cryptographic Authentication", Proceedings of the Symposium on Security and Privacy, IEEE Comp. Soc. Press, ISBN 0-8186-1939-2, (May 1989),	
	✓	HP MOBILE SECURITY OVERVIEW, "HP Mobile Security Overview", (Sept. 2002), 1-10	
	✓	IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991), 156-158	
	✓	IBM CORPORATION, "IBM ThinkPad T30 Notebooks", IBM Product Specification, located at www-1.ibm.com/services/files/cisco_130_spec_sheet_070202.pdf , last visited June 23, 2004, (July 2, 2002), 1-6	
	✓	INTEL, "IA-32 Intel Architecture Software Developer's Manual", Volume 3: System Programming Guide, Intel Corporation - 2003, 13-1 through 13-24	

EXAMINER

ELF

DATE CONSIDERED

18 MAR '05

(Substitute Disclosure Statement Form (PTO-1449))

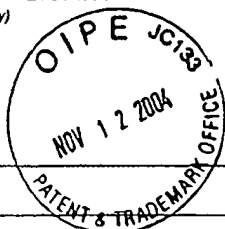
* EXAMINER: Initial if reference considered, whether or not citation is to conform with MPEP 608. Draw the checkmark if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional) Applicant is to place a check mark here if English language Translation is attached

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)



Complete if Known

Application Number	09/540,613
Filing Date	March 31, 2000
First Named Inventor	Ellison, Carl
Group Art Unit	Unknown
Examiner Name	Tran, Ellen

Sheet 2 of 2

Attorney Docket No: 42P08628

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
ECT	/	INTEL CORPORATION, "Intel 82802AB/82802AC Firmware Hub (FWH)", Intel Product Datasheet, Document Number 290658-004, (November 2000), 1-6, 17-28	
	/	KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19	
	/	KASHIWAGI, KAZUHIKO, et al., "Design and Implementation of Dynamically Reconstructing System Software", Software Engineering Conference, Proceedings 1996 Asia-Pacific Seoul, South Korea 4-7 Dec. 1996, Los Alamitos, CA USA, IEEE Comput. Soc, US, ISBN 0-8186-7638-8, (1996),	
	/	LUKE, JAHN, et al., "Replacement Strategy for Aging Avionics Computers", IEEE AES Systems Magazine, XP002190614, (March 1999),	
	/	MENEZES, ALFRED J., et al., "Handbook of Applied Cryptography", CRC Press LLC, USA XP002201307, (1997), 475	
	/	RICHT, STEFAN, et al., "In-Circuit-Emulator Wird Echtzeitauglich", Elektronik, Franzis Verlag GMBH, Munchen, DE, Vol. 40, No. 16, XP000259620, (100-103), 8-6-1991	
	/	ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", Proceedings of the 9th USENIX Security Symposium, XP002247347, Denver, Colorado, (8/14/00), 1-17	
	/	SAEZ, SERGIO, et al., "A Hardware Scheduler for Complex Real-Time Systems", Proceedings of the IEEE International Symposium on Industrial Electronics, XP002190615, (July 1999), 43-48	
	/	SCHNEIER, BRUCE, "Applied Cryptography: Protocols, Algorithm, and Source Code in C", Wiley, John & Sons, Inc., XP002939871; ISBN 0471117099, (Oct. 1995), 47-52	
V	/	SHERWOOD, TIMOTHY, et al., "Patchable Instruction ROM Architecture", Department of Computer Science and Engineering, University of California, San Diego, La Jolla, CA, (Nov. 2001),	

EXAMINER

DATE CONSIDERED

18 MAR '05

Substitute Disclosure Statement Form (PTO-1449)

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.